



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/933,720	08/22/2001	Robert Lambert	06944.0047	6274

27155 7590 05/20/2004

MCCARTHY TETRAULT LLP
SUITE 4900, P.O. BOX 48
66 WELLINGTON ST. WEST
TORONTO, ONTARIO, M5K 1E6
CANADA

EXAMINER

TRUONG, THANHNGA B

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 05/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/933,720

Applicant(s)

LAMBERT ET AL.

Examiner

Thanhnga Truong

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 August 2001.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-27 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-27 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 22 August 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 4.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-18 are rejected under 35 U.S.C. 102(e) as being anticipated by Kaliski, Jr. et al (US 5,854, 759).

a. Referring to claim 1:

i. Kaliski teaches:

(1) transmitting an element represented in a first basis from a first correspondent to an intermediate processor; converting the transmitted element into a second basis representation by said intermediate processor to produce a converted element [i.e., referring to Figure 1, the basis converter 12 is configured to support an export operation, that is, the conversion of an internal basis representation A to an external basis representation B. The externally shifted sequence generator 14 receives an internal basis representation A via input 18 (column 10, lines 27-32). The processor 22 may be a microprocessor, central processing unit (CPU), application-specific integrated circuit (ASIC) or any other suitable digital data processor. The basis converter 12 and the elements thereof may be configured as software modules executed by the processor 22, as separate dedicated hardware modules, or as various combinations of software and hardware. For example, both the externally shifted sequence generator 14 and extractor 16 may be embodied partially or completely in software executed by the processor 22 (column 10, lines 51-60)];

(3) forwarding said converted element to the first correspondent [i.e., **Figure 13 shows an enhanced finite field arithmetic unit 160 which includes basis conversion capabilities. The enhanced arithmetic unit 160 includes the import basis converter 152 and is rotate/extract basis converter 154 described in conjunction with Figure 12, as well as a finite field arithmetic unit 162 such as the arithmetic unit 50 of Figure 4. The enhanced arithmetic unit 160 supports finite field arithmetic operations in an internal basis as well as an additional basis, and may include more than the one set of basis converters shown, whereby “forwarding said converted element to the first correspondent” is considered to include in this arithmetic operations (column 16, lines 56-66));** and

(4) operating on said converted element by said first correspondent in a cryptographic operation [i.e., **Figure 14 illustrates that the enhanced arithmetic unit 160 may be coupled to a cryptographic processor 170 in order to support cryptographic operations in multiple bases. Numerous other applications of the rotate/extract basis converter of Kaliski are also possible (column 17, lines 1-5)].**

b. Referring to claim 2:

i. This claim has limitations that is similar to those of claim 1 (4), thus it is rejected with the same rationale applied against claim 1 (4) above.

c. Referring to claim 3:

i. Kaliski further teaches:

(1) wherein said result is a signature [i.e., **referring to Figure 14, “signature” is considered to include in cryptographic processor 170)].**

d. Referring to claim 4:

i. Kaliski further teaches:

(1) transmitting said converted element by said intermediate processor to said second correspondent [i.e., **Figure 12 shows a basis converter 150 which includes an import basis converter 152 and a rotate/extract basis converter 154. The import basis converter receives a first basis**

representation as an input, and converts the first basis representation to an internal basis representation using operations in the internal basis. The rotate/extract basis converter 154 converts the internal basis representation to a second basis representation (column 16, lines 46-53)].

e. Referring to claim 5:

i. This claim has limitations that is similar to those of claims 1 (4) and 4, thus it is rejected with the same rationale applied against claims 1 (4) and 4 above.

f. Referring to claims 6-9:

i. Kaliski further teaches:

(1) wherein said converted element is a short term public key and long term public key; wherein one of said correspondents is a low power computing device, a smartcard [i.e., many public-key cryptosystems are based on operations in large finite mathematical groups, and the security of these cryptosystems relies on the computational intractability of computing discrete logarithms in the underlying groups, "a short term public key and long term public key, and smartcard" are considered to produce via these cryptosystems (column 35, lines 29-32)].

g. Referring to claim 10:

i. Kaliski further teaches:

(1) wherein said cryptographic operation employs an elliptic curved scheme [i.e., many public-key cryptosystems are based on operations in large finite mathematical groups, and the security of these cryptosystems relies on the computational intractability of computing discrete logarithms in the underlying groups. Two major classes of such cryptosystems are conventional discrete logarithm cryptosystems and elliptic curve cryptosystems (column 35, lines 29-35)].

h. Referring to claim 11:

i. Kaliski further teaches:

(1) wherein said intermediate processor is a Certifying Authority [i.e., referring to Figure 1, the processor 22, that is “a Certifying Authority”].

i. Referring to claim 12:

i. Kaliski teaches:

(1) transmitting an element represented in a first basis from a first correspondent to an intermediate processor [i.e., referring to Figure 1, the basis converter 12 is configured to support an export operation, that is, the conversion of an internal basis representation A to an external basis representation B. The externally shifted sequence generator 14 receives an internal basis representation A via input 18 (column 10, lines 27-32). The processor 22 may be a microprocessor, central processing unit (CPU), application-specific integrated circuit (ASIC) or any other suitable digital data processor. The basis converter 12 and the elements thereof may be configured as software modules executed by the processor 22, as separate dedicated hardware modules, or as various combinations of software and hardware. For example, both the externally shifted sequence generator 14 and extractor 16 may be embodied partially or completely in software executed by the processor 22 (column 10, lines 51-60)];

(2) transmitting of a second element represented in a second basis from a second correspondent to said intermediate processor [i.e., referring to Figure 13, the enhanced arithmetic unit 160 supports finite field arithmetic operations in an internal basis as well as an additional basis, and may include more than the one set of basis converters shown, whereby “transmitting of a second element represented in a second basis from a second correspondent to said intermediate processor” is considered to include in these arithmetic operations (column 16, lines 56-66)];

(3) converting the transmitted first element into said second basis representation by said intermediate processor to produce a first converted element; forwarding said first converted element to said second correspondent [i.e., Figure 12 shows a basis converter 150 which includes an import basis converter

152 and a rotate/extract basis converter 154. The import basis converter receives a first basis representation as an input, and converts the first basis representation to an internal basis representation using operations in the internal basis. The rotate/extract basis converter 154 converts the internal basis representation to a second basis representation (column 16, lines 46-53)];

(4) converting the transmitted second element into a first basis representation by said intermediate processor to produce a second converted element; forwarding said second converted element to said first correspondent [i.e., **Figure 13 shows an enhanced finite field arithmetic unit 160 which includes basis conversion capabilities. The enhanced arithmetic unit 160 includes the import basis converter 152 and is rotate/extract basis converter 154 described in conjunction with Figure 12, as well as a finite field arithmetic unit 162 such as the arithmetic unit 50 of Figure 4. The enhanced arithmetic unit 160 supports finite field arithmetic operations in an internal basis as well as an additional basis, and may include more than the one set of basis converters shown (column 16, lines 56-66)].**

j. Referring to claims 13-14:

i. Kaliski further teaches:

(1) operating on said second converted element by said first correspondent in a cryptographic operation to produce a result and a second result [i.e., **referring to Figure 14, a cryptographic processor 170, that is for “operating on said second converted element by said first correspondent in a cryptographic operation to produce a result and a second result”].**

k. Referring to claims 15-17:

i. These claims have limitations that is similar to those of claims 6 and 7, thus they are rejected with the same rationale applied against claims 6 and 7 above.

l. Referring to claim 18:

i. This claim has limitations that is similar to those of claim 10, thus it is rejected with the same rationale applied against claim 10 above.

3. Claims 19-24 is rejected under 35 U.S.C. 102(e) as being anticipated by Lenstra (US 6,446, 205).

a. Referring to claim 19:

i. Lenstra teaches:

(1) representing a first field element in terms of a first basis; computing a first function of a first sequence of traces of said first field element; and using said first sequence of traces as said bit string [i.e., referring to Figure 5, at step 505, the value for security parameter B and mapping functions R1, R2, R3 are obtained. At step 510, the participant's cryptosystem selects vaules for security parameters Bs and Bb. At step 515, the participant's cryptosystem randomly selects a bitstring s having Bs bits, that is for "computing a first function of a first sequence of traces of said first field element; and using said first sequence of traces as said bit string". At step 520, the participant's cryptosystem applies the mapping functions R1 and R2 to the concatenation of its identify ID and the bitstring s to obtain two positive B-bit integers $a=R1(ID||s)$ and $b0=R2(ID||s)$, that is for "first field element and second field element", and also initializes an integer b1, $b1=0$ (column 6, lines 62-67 through column 7, lines 1-3)].

b. Referring to claims 20-22:

i. These claims have limitations that is similar to those of claim 19, thus they are rejected with the same rationale applied against claim 19 above.

c. Referring to claim 23:

i. Lenstra teaches:

(1) using said bit string as a shared secret in a cryptographic scheme between a first correspondent and a second correspondent [i.e., as shown in Figure 4, parties wishing to communicate exchange cryptographic data, reconstruct each other's public key data, and then use the reconstructed keys in cryptographic protocols, such as a signature scheme or data encryption/decryption scheme (column 3, lines 57-61)].

d. Referring to claim 24:

i. Lenstra teaches:

(1) wherein said cryptographic scheme is an elliptic curved scheme [i.e., **Lenstra's invention relates to elliptic curve cryptosystems in which each participant chooses its own elliptic curve, from a predetermined set of elliptic curve equations, and also chooses its own finite field (column 3, lines 14-17)]**].

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lenstra, and further in view of Kaliski, Jr. et al.

a. Referring to claims 25-27:

i. Lenstra teaches the claimed subject matter except for:

(1) wherein said first function is an irreducible polynomial of degree N; wherein said second function is an irreducible polynomial of degree N; and wherein said first field element is converted in terms of said second basis by finding a root for said polynomial for said first basis in a representation generated by said second basis; and evaluating said polynomial representing said first field element in said first basis at said root.

ii. However, Kaliski teaches:

(1) two common types of basis are polynomial basis and normal basis. In a polynomial basis, the basis elements are successive powers of an element γ , call the generator: $\omega_i = \gamma^i$. The element γ must satisfy certain properties, namely that the powers $\gamma^0, \dots, \gamma^{m-1}$ are linearly independent. A polynomial f of degree m , called the minimal polynomial of γ , relates the successive powers, so that

$\gamma^m = f^{m-1} \gamma^{m-1} + f^{m-2} \gamma^{m-2} + \dots + f^1 \gamma^1 + f^0 \gamma^0$. Such a polynomial f must be irreducible over the ground field $GF(q)$ (column 2, lines 17-32). Furthermore, The algorithms may be used to convert from a polynomial basis to a normal basis, from a normal basis to a polynomial basis, from a polynomial basis with one generator to a polynomial with another generator, or from a normal basis with one generator to a normal basis with another generator, to give a few examples (column 6, lines 1-5).

iii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include the polynomial basis representation as in Lenstra's cryptosystem since it is a common choice of basis for representing elements of the finite field (**column 1, lines 22-23 of Kaliski**).

iv. The ordinary skilled person would have been motivated to:

(1) include the polynomial basis representation as in Lenstra's cryptosystem for a variety of reasons, including cost, performance, and compatibility with other applications, implementations of $GF(2^m)$ arithmetic vary in their choice of basis (**column 1, lines 25-28 of Kaliski**).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Vanstone et al (US 6, 141, 420) discloses an elliptic curve encryption system represents coordinates of a point on the curve as a vector of binary digits in a normal basis representation in F_{2^m} . A key is generated from multiple additions of one or more points in a finite field (see abstract).

b. Yin et al (US 6, 389, 442 B1) The invention provides improved techniques for multiplication of signals represented in a normal basis of a finite field. An illustrative embodiment includes a first rotator which receives a first input signal representative of a first normal basis field element ($a_0 a_1 \dots a_{m-1}$), and

a second rotator which receives a second input signal representative of a second normal basis field element (b.sub.0 b.sub.1 . . . b.sub.m-1) (see abstract).


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TBT

May 11, 2004


KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2135